REMARKS

This paper is submitted in response to the Final Office Action dated December 8, 2009 (the "Final Office Action").

Claims 39-40, 44-47, 49-57, 59-62, 64-65, 67, and 71-74 are pending in the application.

Claims 39-40, 44-47, 49-57, 59-62, 64-65, 67, and 71-74 stand rejected.

The amendments add no new matter. Support for the amendments may be found throughout Applicant's Specification and Drawings as originally filed, for example on p. 3, lines 6-8; p. 4, lines 10-12; and p. 4, lines 23-24. While not conceding that the cited reference(s) qualify as prior art, but instead to expedite prosecution, Applicant has chosen to respond as follows. Applicant reserves the right to establish that the cited reference(s), or other references cited thus far or hereafter, do not qualify as prior art as to an invention embodiment previously, currently, or subsequently claimed. Applicant also reserves the right, for example in a continuing application, to pursue the previously pending claims or claims similar thereto. Applicant respectfully submits that the pending claims are allowable in view of the following remarks and the above amendments, and respectfully requests reconsideration of the pending rejections.

1. Rejections of claims under 35 U.S.C. § 103(a)

Claims 39-40, 44-47, 49-57, 59-62, 64-65, 67, and 71-74 stand rejected under § 103(a) as purportedly being unpatentable over U.S. Patent No. 6,870,921 issued to Elsey et al. ("**Elsey**") in view of an article by Thomas, "Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments," *Proceedings of the second ACM workshop on Role-based access control*, pp. 13-19 (1997) ("**Thomas**"), and in view of an article by Sandhu et al., "The NIST Model for Role-Based Access Control: Towards A Unified Standard," 17 pp., provided by the Examiner and cited by the Examiner as pp. 47-63 of the *Proceedings of the fifth ACM workshop on Role-based access control*, ACM (2000) ("**Sandhu**"). Applicant respectfully submits that the amended claims are allowable under § 103(a) because the cited portions of the reference do not disclose or fairly suggest each limitation of Applicant's claims.

Applicant gratefully acknowledges the Examiner's expanded discussion of the currently pending independent claims in the Response to Arguments section and elsewhere in the Final Office Action. Nonetheless, Applicant respectfully requests reconsideration in view of the following observations.

Applicant notes that the following observations stand alone, independent of the above-noted amendments to various dependent claims. For example, independent claim 39 has not been amended in this paper.

Claim 39 includes an access control subsystem. The access control subsystem is configured to provide a user with access to files in a first virtual database, but *only when* the user has an access authorization to that first virtual database. Claim 39 recites that this access authorization is from a first tenant that corresponds to the first virtual database. Moreover, claim 39 recites that the access control subsystem is configured to *deny a second access to at least one other virtual database when the user has the access authorization to the first virtual database*. Moreover, that other virtual database is one that:

> *corresponds to at least one tenant other than the first tenant.*

The Final Office Action cites Sandhu with regard to this limitation. Sandhu relates to the National Institute of Standards and Technology (NIST) models of role-based access control (RBAC). *See* Sandhu, § 2, lines 2-7; § 2, lines 2-19. With regard to the *tenant other than the first tenant*, the Final Office Action cites the following passage:

> 7.8 RBAC administration
>
> The NIST RBAC model does not specify the authorization for assigning users to roles, permissions to roles and roles to roles (in a role hierarchy), and for revoking these assignments. Several models for this purpose have been proposed in the literature. Some of these are rooted in traditional discretionary access control where the owner of a role[ ] is allowed full control over that role. Others centralize administrative authority in a single security officer role. A decentralized administrative model based on administrative roles has been recently published. Due to lack of consensus in this arena the NIST RBAC model does not incorporate an administrative component.

Sandhu, § 7.8 (citation omitted). This passage teaches that various administrative operations can be centralized or decentralized in an RBAC system. But this passage provides no details on any preferred features of a system with decentralized administrative operations.

The Final Office Action appears to argue that Sandhu's reference to a "decentralized administrative model" meets the above noted limitations of claim 29. Applicant respectfully disagrees. Sandhu does not teach what it means for an RBAC model to be "decentralized," other than implying that such a system does not place the administrative authority "in a single security officer role." In particular, Sandhu does not teach, or even suggest, that users of one administrator's resources should be "den[ied] access" to other administrators' resources.

The Final Office Action appears to equate Sandhu's "administrative roles" with the *first tenant* and the *at least one other tenant* in Applicant's claim 29. Even if this characterization of Sandhu were appropriate (a point which Applicant does not concede), Sandhu fails to disclose that access corresponding to one administrator should be restricted due to a grant of access by another administrator. No restriction from one administrator's resources is denied in Sandhu because of access that has been granted to another administrator's resources. More generally, Sandhu is altogether silent regarding any particular implementations or specific rules that would be used in the decentralized administrative model. This silence does not portend Applicant's claim limitations.

Specifically, the cited passages of Sandhu fail to disclose an access control subsystem that is configured to *deny a second access* to at least *one other virtual database that corresponds to at least one tenant other than the first tenant* while the user has the access authorization to the first tenant's virtual database, as recited in Applicant's claim 39.

Indeed, Sandhu's static separation of duties is incongruous with these limitations of claim 39. The Final Office Action appears to equate Sandhu's static separation of duties (introduced in §§ 5.1) with a denial of access. Sandhu' teaches that this model:

> enforce[s] constraints on the assignment of users to roles. This means that if a user is authorized as a member of one role, the user is prohibited from being a member of a second role.

See Sandhu, § 5.1, lines 4-10. This model places restrictions on the roles that a user can take at one time: the user is prohibited from simultaneously taking conflicting roles, such as Billing

Clerk and Accounts Receivable Clerk (§ 5.1). But this model does not require that the mutually exclusive roles are based on the administrative roles (§ 7.8) cited by the Final Office Action.

More to the point, Sandhu's static separation of duties does not impose restrictions that are based on *the tenant* of a resource. (Indeed, it is not clear who that tenant would be in Sandhu's models, which highlights Applicant's previous arguments regarding the incongruity of Sandhu.[1]) Even if it could be argued that Sandhu's Billing Clerk and Accounts Receivable Clerk operate at a company that transmits and receives bills to various business partners, and that these business partners correspond to the *first tenant* and the *at least one other tenant* in Applicant's claim 29 (a point which Applicant does not concede), Sandhu altogether fails to teach that the separation of duties should be based on the identity of those business partners. For example, Sandhu certainly does not teach that Billing Clerk should be denied access to Company X's records during the time that Billing Clerk has access to Company Y's records.

At least for these reasons, Sandhu's discussion of a decentralized administrative model fails to teach an access control subsystem that is configured to *deny a second access* to at least *one other virtual database that corresponds to at least one tenant other than the first tenant* when the user has the access authorization to the first tenant's virtual database, as recited in Applicant's claim 39. Applicant also does not find these limitations in other cited passages of Sandhu, or in the cited passages of Elsey and Thomas, whether taken individually or in combination with each other and the knowledge available to a skilled person. At least for this reason, independent claim 39 and all claims dependent thereon are additionally allowable under § 103(a). At least for similar reasons, independent claims 46 and 64 and all claims dependent thereon are also allowable under § 103(a).

---

[1] Moreover, as Applicant has previously explained, Sandhu's example of a dynamic separation of duties (§ 5.2) further highlights the incongruity of this reference. In that example, Sandhu prohibits a single user from simultaneously acting as a Cashier and as a Cashier supervisor while accessing a particular recourse—a cash drawer—to avoid conflicts of interest between these two roles. Even if this resource of a cash drawer could be equated with the virtual databases in claim 39 (a point which Applicant does not concede), Sandhu's teachings regarding this cash drawer are not even remotely analogous to the relationships recited in claim 39. Sandhu's sharing of a single resource (the cash drawer) is counter to the allowed and denied accesses in claim 39, which apply to different resources. Sandhu denies simultaneous access–by multiple roles–to a single resource (the cash drawer) unless the roles are played by more than one users.

In contrast, claim 39 denies simultaneous access–by a single user–to multiple resources (virtual databases). Access is allowed to files in a first virtual database corresponding to a first tenant, and access is denied to a virtual database that corresponds to at least one tenant other than the first tenant. This denial of access to multiple resources is not at all paralleled by the relationships in the cited passages of Sandhu.

2. Additional patentability of amended dependent claims.

In addition to the above-noted comments on the patentability of the already-examined non-amended claims, Applicant has amended dependent claims 73 and 74 in an effort to further prosecution.

As amended, claim 73 recites that the access control subsystem is configured to *deny access to each virtual database . . . other than the first virtual database*. This denial applies *while the user has the access authorization to the first virtual database*. These limitations are absent from the cited passages.

Indeed, Sandhu's teachings are directly counter to these limitations. Sandhu's RBAC systems are described in four "levels" or versions, including a basic "Flat RBAC" model. *See* Sandhu, § 2, lines 11-15; § 2.1. "Each level adds exactly one new requirement," and includes the requirements of the previous levels. *See* Sandhu, § 2, lines 13-16.

The basic Flat RBAC model "requires that users can simultaneously exercise permissions of multiple roles. This precludes products that restrict users to activation of only one role at a time." *See* Sandhu, §2.1, lines 15-18. This requirement is inherited by all three of Sandhu's other levels in the NIST RBAC model. *See* Sandhu, § 2, lines 13-15; §3, col. 4, lines 12-13. Sandhu makes clear that this requirement is not optional, and explicitly teaches against models that lack this requirement. Sandhu teaches that a feature that fails this requirement by limiting users to a single role in a session "is considered overly restrictive." *See* Sandhu, §3, col. 3, line 14.

In contrast, Applicant's claim 73 explicitly recites that the access control subsystem is configured to *deny access to each virtual database . . . other than the first virtual database while the user has the access authorization to the first virtual database*. These limitations are absent from the cited passages, and would not be found in a combination of the cited references in view of Sandhu's teaching to the contrary.

At least for these reasons, amended claim 73 is additionally patentable under § 103(a). At least for similar reasons, amended claim 74 is also additionally patentable under § 103(a).

CONCLUSION

In view of the amendments and remarks set forth herein, the application and the claims therein are believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the Examiner is invited to telephone the undersigned at 512-439-5097.

If any extensions of time under 37 C.F.R. § 1.136(a) are required in order for this submission to be considered timely, Applicant hereby petitions for such extensions. The undersigned hereby authorizes that any fees due for such extensions or any other fee associated with this submission, as specified in 37 C.F.R. §§ 1.16 or 1.17, be charged to deposit account no. 502306.

I hereby certify that this correspondence is being submitted to the U.S. Patent and Trademark Office in accordance with 37 C.F.R. § 1.8 on February 8, 2010 (CDT) by being (a) transmitted via the USPTO Electronic Filing System; or (b) transmitted by facsimile to 571-273-8300; or (c) deposited with the U.S. Postal Service as First Class Mail in an envelope with sufficient postage addressed to: Mail Stop AF, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia, 22313-1450.

/ Cyrus F. Bharucha / — Cyrus F. Bharucha

February 8, 2010 — Date

Respectfully submitted,

/ Cyrus F. Bharucha /

Cyrus F. Bharucha
Attorney for Applicant
Reg. No. 42,324
512-439-5097
512-439-5099 (fax)